Journal of the Iranian Mathematical Society
Vol. 1 No. 2 (2020), pp. 157-161.

A NOTE ON FACTORIZATIONS OF FINITE GROUPS

GEORGE M. BERGMAN

Communicated by Alireza Abdollahi

Abstract. In Question 19.35 of the Kourovka Notebook, M. H. Hooshmand asks whether, given a finite group G and a factorization $\mathrm{card}(G) = n_1 \dots n_k$, one can always find subsets $A_1, \dots, A_k$ of G with $\mathrm{card}(A_i) = n_i$ such that $G = A_1 \dots A_k$; equivalently, such that the group multiplication map $A_1 \times \dots \times A_k \to G$ is a bijection.

We show that for G the alternating group on 4 elements, $k = 3$, and $(n_1, n_2, n_3) = (2, 3, 2)$, the answer is negative. We then generalize some of the tools used in our proof, and note a related open question.

1. The example.

In this section we develop the example described in the Abstract.

Definition 1.1 (after [4, §1], cf. [6, p. 6]). *Suppose G is a group, k is a positive integer, and $A_1, \dots, A_k$ are subsets of G. In this situation, if the multiplication map $A_1 \times \dots \times A_k \to G$ is bijective, we shall write $G = A_1 \cdot \dots \cdot A_k$, and call this a ($k$-fold)* factorization *of G.*

(*If G is finite, we see that the above bijectivity condition can alternatively be expressed, as in* [1, Question 19.35]*, by the conditions $G = A_1 \dots A_k$, and* $\mathrm{card}(G) = \mathrm{card}(A_1) \dots \mathrm{card}(A_k)$.)

MSC(2020): Primary: 20D60.

Keywords: Factorization of a finite group; product of subsets.

Received: 18 May 2020, Accepted: 14 June 2020.

Archived at http://arXiv.org/abs/2003.12866. After publication, any updates, errata, related references, etc., found will be recorded at http://math.berkeley.edu/~gbergman/papers/ .

Observe that if $G = A_1 \cdot \ldots \cdot A_k$ is a k-fold factorization of G, then for $1 \leq j < k$, $G = (A_1 \ldots A_j) \cdot (A_{j+1} \ldots A_k)$ is a 2-fold factorization. Though the example we are working toward is a 3-fold factorization, the key to its proof will be a property of 2-fold factorizations, namely

Lemma 1.2 (cf. [5, Cor. 2.14(a)]). *Let $G = A \cdot B$ be a factorization of a finite group. Then the order of the subgroup of G generated by A is a multiple of* $\mathrm{card}(A)$, *and the order of the subgroup generated by B is a multiple of* $\mathrm{card}(B)$.

Proof. Let H be the subgroup of G generated by A. For each $b \in B$, the set $A\,b$ is contained in a single right coset of H; hence every right coset of H is a disjoint union of sets of cardinality $\mathrm{card}(A)$, hence $\mathrm{card}(H)$ is a multiple of $\mathrm{card}(A)$. The statement about the subgroup generated by B is seen in the same way. □

We will also use the following observation.

Lemma 1.3 (after [4]). *If $G = A_1 \cdot \ldots \cdot A_k$ is a factorization of a group G, then for all $g, h \in G$, $(g\,A_1) \cdot A_2 \cdot \ldots \cdot A_{k-1} \cdot (A_k\,h)$ is also a factorization of G.*

Hence if for some positive integers $n_1, \ldots, n_k$, G has a k-fold factorization with $\mathrm{card}(A_i) = n_i$ $(i = 1, \ldots, k)$, it has such a factorization in which A_1 and A_k both contain the identity element e. □

We can now prove

Proposition 1.4. *Let G be the alternating group on 4 elements, a group of order 12. Then G has no factorization $A_1 \cdot A_2 \cdot A_3$ with* $(\mathrm{card}(A_1), \mathrm{card}(A_2), \mathrm{card}(A_3)) = (2, 3, 2)$.

Proof. Recall that the elements of exponent 2 in G form a normal subgroup $N \cong Z_2 \times Z_2$, that G is an extension of N by a group of order 3 whose action by conjugation cyclically permutes the three proper nontrivial subgroups of N, and that all elements of G not in N have order 3.

Suppose $G = A_1 \cdot A_2 \cdot A_3$ were a factorization with $\mathrm{card}(A_1) = 2$, $\mathrm{card}(A_2) = 3$, $\mathrm{card}(A_3) = 2$. By Lemma 1.3 we can assume without loss of generality that A_1 and A_3 have the forms $\{e, g\}$ and $\{e, h\}$ respectively. The orders of the groups these sets generate are the orders of g and h, and by Lemma 1.2, are even. But the only elements of G of even order have order 2, hence A_1 and A_3 are in fact subgroups (which may or may not be distinct).

Since A_1 and A_3 are contained in N, for $G = A_1\,A_2\,A_3$ to hold, A_2 must contain representatives of all three cosets of N in G. Moreover, elements of G act transitively on the set of 2-element subgroups of N; so A_2 must contain an element g that conjugates A_1 to A_3.

Hence when we multiply out $A_1\,A_2\,A_3$, the result contains $A_1\,g\,A_3 = g\,A_3\,A_3$. But the multiplication map $A_3 \times A_3 \to A_3$ is not one-to-one; from which we see that the multiplication map $A_1 \times A_2 \times A_3 \to G$ cannot be one-to-one, contradicting the definition of a factorization. □

This completes our negative answer to [1, Question 19.35] for $k = 3$. What about larger k? If we allow factorizations with some factors equal to 1, then for any k, a negative example with cardinalities $n_1, \ldots, n_k$ yields negative examples for all $k' > k$, by keeping the same G and $n_1, \ldots, n_k$, and taking

$n_{k+1} = \ldots = n_{k'} = 1$; so the only remaining open case is $k = 2$. However, Hooshmand (personal correspondence) has indicated that he intended only factorizations of $\mathrm{card}(G)$ into factors > 1. With that restriction, the problem remains open for all $k > 3$; I do not know whether there is an easy way to modify the present example to cover those cases.

Hooshmand posed the question for $k = 2$ in [3], and refers to that case in [1] as of particular interest; his preprint [4] concerns that case, and also mentions the case $k > 3$ at the end, as Problem IV. The case $k = 2$ is also studied in [2], after a discussion of the history of the subject of group factorizations.

2. Strengthening our lemmas

In the context of Lemma 1.2, the order of the subgroup H of G generated by A can change on left-multiplying A by an element $g \in G$, a fact we implicitly used when we applied Lemma 1.3 in the proof of Proposition 1.4. In the next result, modified versions of that subgroup are noted whose orders are not so affected. Also, while Lemma 1.2 is applicable only to the first and last sets A_1 and A_k in a factorization $G = A_1 \cdot \ldots \cdot A_k$, part (iii) below obtains a similar, though weaker, condition on the cardinalities of the other A_i. (This will be slightly improved in Lemma 2.3.)

Lemma 2.1. *Let $A_1 \cdot \ldots \cdot A_k$ be a factorization of a finite group G. Then*

(i) $\mathrm{card}(A_1)$ *divides the order of the subgroup of G generated by the set $A_1^{-1}A_1 = \{g^{-1}h \mid g, h \in A_1\}$, which can also be described as generated by any one of the subsets $g^{-1}A_1$ $(g \in A_1)$. Moreover, that order is also the order of the subgroup generated by $A_1\,A_1^{-1} = \{g\,h^{-1} \mid g, h \in A_1\}$, equivalently, by any of the subsets $A_1\,g^{-1}$ $(g \in A_1)$.*

(ii) *Similarly,* $\mathrm{card}(A_k)$ *divides the order of the subgroup of G generated by $A_k\,A_k^{-1}$, equivalently, by any of the subsets $A_k\,g^{-1}$ $(g \in A_k)$, and that order is also the order of the subgroup generated by $A_k^{-1}A_k$, equivalently, by any of the subsets $g^{-1}A_k$ $(g \in A_k)$.*

(iii) *For $1 < i < k$,* $\mathrm{card}(A_i)$ *divides the order of the* normal subgroup *of G generated by $A_i^{-1}A_i$, equivalently, by any of the subsets $g^{-1}A_i$ $(g \in A_i)$, equivalently, by $A_i\,A_i^{-1}$, or by any of the subsets $A_i\,g^{-1}$ $(g \in A_i)$.*

Proof. (i) Combining Lemma 1.2 and Lemma 1.3, we see that for every $g \in A_1$, $\mathrm{card}(A_1)$ divides the order of the group generated by $g^{-1}A_1$ (the argument that we implicitly used in the proof of Proposition 1.4). Moreover, given g, $g' \in A_1$, the group generated by $g^{-1}A_1$ will contain $(g^{-1}g')^{-1}(g^{-1}A_1) = g'^{-1}A_1$; so the groups generated by $g^{-1}A_1$ are the same for all $g \in A_1$. Clearly their common value can also be described as the group generated by $A_1^{-1}A_1$, so the groups named in the first sentence of (i) are indeed equal.

The groups in the second sentence of (i) are equal to one another by the same argument. Moreover, for any $g \in A_1$, $A_1\,g^{-1} = g\,(g^{-1}A_1)\,g^{-1}$, so the group generated by $A_1\,g^{-1}$ is conjugate in G to the group generated by $g^{-1}A_1$. Hence the order of the group in the second sentence is the same as that of the group in the first sentence.

(ii) holds by the same reasoning.

(iii) For each i we similarly see that the *not* necessarily normal subgroups generated by the subsets of G named in the first half of (iii) are all equal, and are conjugate to the common value of those generated by the subsets named in the second half. Hence the *normal* subgroups generated by these sets are all equal. Let us call their common value N.

The condition $G = A_1 \cdot \ldots \cdot A_k$ implies that G is the disjoint union of the sets $h\,A_i\,h'$ for $h \in A_1 \ldots A_{i-1},\ h' \in A_{i+1} \ldots A_k$, and clearly each of these sets is wholly contained in one coset of N, namely $h\,N\,h' = hh'\,N = N\,hh'$. Hence N (and, indeed, every coset of N) is the disjoint union of a family of such sets, so N indeed has order a multiple of $\mathrm{card}(A_i)$. □

We also note an easy strengthening of Lemma 1.3.

Lemma 2.2. *If $A_1 \cdot \ldots \cdot A_k$ is a factorization of a group G, then for all $g_0, g_1, \ldots, g_k \in G$, $(g_0^{-1} A_1\, g_1) \cdot (g_1^{-1} A_2\, g_2) \cdot \ldots \cdot (g_{k-1}^{-1} A_k\, g_k)$ is also a factorization of G.*

In particular, if for some positive integers $n_1, \ldots, n_k$, G has a k-fold factorization with $\mathrm{card}(A_i) = n_i$ $(i = 1, \ldots, k)$, then it has such a factorization in which all A_i contain e. □

A choice of $k+1$ elements $g_0, \ldots, g_k$ as above actually gives one more degree of freedom than is needed to make all the A_i contain e. This might be used to replace some particular term by a chosen conjugate of itself.

Returning to Lemma 2.1, one may ask whether in statement (iii) thereof one can replace "normal subgroup" by "subgroup", as in (i) and (ii). Not as far as I can see. For though G is the disjoint union of the sets $h\,A_i\,h'$ referred to in the proof of (iii), these lie in cosets of different conjugates of H; namely, $h\,A_i\,h'$ lies in a right coset of $h\,H\,h^{-1}$ (and also in a left coset of $h'^{-1} H\,h'$), and such conjugates in general partially overlap one another, so we can't get a nice decomposition of any one of these cosets from our hypotheses.

The result (iii) is very weak; e.g., if G is a simple group, it tells us nothing that isn't evident from the definition of $A_1 \cdot \ldots \cdot A_k$ being a factorization of G. We give below a somewhat stronger, if not as easy to state, result. To keep the statement from being too complicated, we shall not use the "strengthening" gotten by replacing the sets in our factorization by translates containing e, but simply understand that if this is desired, it can be achieved by combining the result as stated with Lemma 2.2.

Lemma 2.3. *In the context of Lemma 2.1(iii), let K, H and K' be, respectively, the subgroups of G generated by $A_1 \ldots A_{i-1}$, by A_i, and by $A_{i+1} \ldots A_k$. Then $\mathrm{card}(A_i)$ divides the order of the subgroup M of G generated by the conjugates of H by all members of K, and also the order of the subgroup M' generated by the conjugates of H by all members of K'.*

Proof. As before, G is the disjoint union of the sets $h\,A_i\,h'$ for $h \in A_1 \ldots A_{i-1},\ h' \in A_{i+1} \ldots A_k$. Now $h\,A_i\,h' \subseteq h\,M\,h'$, which can be rewritten as $M\,h\,h'$ because M is normalized by $h \in K$. So each set $h\,A_i\,h'$ lies wholly in one right coset of M; so each right coset of M is a disjoint union of sets of cardinality $\mathrm{card}(A_i)$, yielding the first of the asserted divisibility statements. The second holds by the analogous reasoning. □

The two conditions on $\mathrm{card}(A_i)$ obtained in the above lemma differ, in general. For instance, if G is a simple group, and we take $k = 3$, let $A_1 = \{e\}$, let A_2 be a proper nontrivial subgroup H of G, and let A_3 be a set of right coset representatives of H in G, then the multiplicative bound on $\mathrm{card}(A_2)$ given by the first assertion is its actual cardinality, while that given by the second is the order of G.

Though I have noted why we cannot expect that in this situation, $\mathrm{card}(A_i)$ will in fact divide $\mathrm{card}(H)$, I don't know a counterexample, so let us record the question. It clearly comes down to

Question 2.4. *If a finite group G has a factorization $G = A_1 \cdot A_2 \cdot A_3$, must $\mathrm{card}(A_2)$ divide the order of the subgroup H of G generated by A_2?*

Acknowledgments

I am indebted to M. H. Hooshmand for posing the interesting question answered in this note, and for correspondence on this material.

References

[1] The Kourovka Notebook, Unsolved problems in group theory, Nineteenth edition. Edited by Victor Mazurov and Evgeny Khukhro, Russian Academy of Sciences Siberian Branch, Sobolev Institute of Mathematics, Novosibirsk, 2018. 248 pp. MR3981599. Readable at https://kourovkanotebookorg.files.wordpress.com/2019/12/19tkt-2.pdf and http://math.nsc.ru/~alglog/19tkt.pdf . Website at https://kourovka-notebook.org/ .

[2] R. Bildanov, V. Goryachenko and A. V. Vasilev, Factoring nonabelian finite groups into two subsets, 7 pages, https://arxiv.org/pdf/2005.12003.pdf.

[3] M. H. Hooshmand, Factor subset of finite group, 2014, https://mathoverflow.net/questions/155986/factor-subset-of-finite-group

[4] M. H. Hooshmand, Basic results for an unsolved problem about factorization of finite groups, to appear.

[5] M. H. Hooshmand, *f*-representatives groups, to appear.

[6] S. Szabó and A. D. Sands, Factoring groups into subsets, Lecture Notes in Pure and Applied Mathematics, 257, CRC Press, 2009, xvi+269 pp. ISBN: 978-1-4200-9046-8. MR2484422. (This work studies factorizations of finite *abelian* groups.)

George M. Bergman

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Email: gbergman@math.berkeley.edu